

UNITED STATES DISTRICT COURT

for the
District of Oregon

FILED 19 APR '19 11:32 USDC-ORP

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 19-mc-341

Sailing Vessel "Mandalay" with Official Number 947859

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Sailing Vessel "Mandalay" with Official Number 947859, presently located at a marine facility on the Multnomah Channel, Portland, Oregon.

located in the _____ District of _____ Oregon _____, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
46 U.S.C. § 70503(a)	Knowingly and Intentionally Possess with Intent to Distribute a Controlled
46 U.S.C. § 70506(a) and (b)	Substance While on Board a Covered Vessel; Conspiracy to Violate Section
	70503

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Todd Clements Special Agent ICE

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone at 11:20 a.m./p.m. (specify reliable electronic means).

Date:

April 19, 2019


Judge's signature

City and state: Portland, Oregon

Honorable Stacie F. Beckerman

Printed name and title

UNITED STATES DISTRICT COURT)
)
DISTRICT OF OREGON)

AFFIDAVIT OF TODD CLEMENTS

**Affidavit in Support of an Application
Under Rule 41 for a Search Warrant**

I, Todd Clements, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) with U.S. Immigration and Customs Enforcement (ICE) and have been so employed since 2003. I am a law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7) and I am authorized by law to conduct investigations and to make arrests for felony offenses. I am currently assigned to the Assistant Special Agent in Charge, Portland, Oregon. From January 2002 through February 2003, I was employed as a Special Agent with the Portland, Oregon District Office of the Immigration and Naturalization Service (INS). Prior to that, I was employed as an Immigration Agent (Enforcement) with the INS Sub-Office in Ventura County, California from June 1998 to January 2002. I am authorized and assigned to investigate violations of federal laws, including 21 U.S.C. §§ 841(a)(1), 846, 848, and 843(b) of the Drug Abuse Prevention and Control Act of 1970; that is, possession with intent to distribute and the distribution of controlled substances, conspiracy to commit such offenses, the operation of a continuing criminal enterprise, and the use of a communication facility to facilitate a felony violation of the Drug Abuse Prevention and Control Act of 1970. During my tenure as a federal law enforcement officer, I have investigated and/or participated in investigations of conspiracy, money laundering, narcotics trafficking, fraud, smuggling and theft. I have also acquired knowledge and information about the illegal drug trade and the various means and methods by which it is

furthered, including through the use of computers, smart phones, digital media and the Internet from formal and informal training, other law enforcement officers and investigators, informants, individuals I have arrested and/or interviewed, and from my participation in other investigations. I have spoken on numerous occasions with suspects, informants, witnesses, as well as law enforcement officers and investigators, concerning the methods and practices of drug traffickers. I have also supervised the activities of informants who provided information and assistance to ongoing drug investigations. I am currently detailed to the High Intensity Drug Trafficking Area (HIDTA) Interdiction Task Force (HIT) located at the Portland Police Bureau's Drugs and Vice Division.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the Sailing Vessel (S/V) Mandalay, Official Number 947859, (hereinafter "**Vessel**") as described in Attachment A hereto, for evidence, contraband, fruits, and instrumentalities for violations of 46 U.S.C. §§ 70503(a) and 70506(a) and (b). As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices, are currently located inside the **Vessel**.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. Title 46, United States Code, Section 70503(a)(1) provides, in relevant part, that while on board a covered vessel, an individual may not knowingly or intentionally possess with intent to distribute a controlled substance. A “covered vessel” means a vessel of the United States or a vessel subject to the jurisdiction of the United States or any other vessel if the individual is a citizen of the United States or a resident alien of the United States. 46 U.S.C. §70503(e). Subsection (a) applies even though the act is committed outside the territorial jurisdiction of the United States. 46 U.S.C. §70503(b). Further, in relevant part, a person violating 46 U.S.C. §70503 may be tried in any district if the offense was begun or committed upon the high seas. 46 U.S.C. §70504(b). A person violating 46 U.S.C. §70503(a)(1) shall be punished as provided in 21 U.S.C. §960. 46 U.S.C. §70506(a). In addition, a person conspiring to violate Section 70503 is subject to the same penalties as provided for violating Section 70503. 46 U.S.C. §70506(b).

Statement of Probable Cause

5. On April 9, 2019, while on routine patrol, United States Coast Guard (USCG) Cutter Alert detected the **Vessel** transiting northbound approximately 225 nautical miles from Newport, Oregon. USCG Cutter Alert was directed to intercept the **Vessel** and conduct right-of-approach questioning. Upon contact, USCG Cutter Alert noted that the **Vessel** had a name “Mandalay”, with a home port of Seattle, Washington, painted on the stern (rear). During the right-of-approach, USCG personnel attempted to communicate with an individual on board the **Vessel**, later determined to be John Phillip Stirling (STIRLING), in person, but STIRLING was not visible and would only communicate with the USCG via radio. During radio communication with USCG, STIRLING claimed Canadian nationality for himself and Canadian registry for the

Vessel. Also during radio communication, STIRLING claimed that the **Vessel's** Canadian flag and Canadian registration documents were lost overboard and that the **Vessel** had been removed from the United States system (registry). USCG personnel subsequently researched ownership and flag-state of the **Vessel** and determined that S/V Mandalay was a United States flagged vessel. Once USCG determined flag-state, a USCG boarding team boarded the **Vessel** on a right-of-visit. Upon boarding the **Vessel**, USCG personnel encountered STIRLING, the sole occupant. During questioning by USCG personnel, STIRLING's speech began to deteriorate until he was only able to communicate in mumbles. USCG personnel, concerned that STIRLING was displaying symptoms of a possible drug overdose, began administering medical treatment to STIRLING. It was later determined that STIRLING needed to be medically evacuated. STIRLING was flown by USCG helicopter to Astoria, Oregon and then taken to Columbia Memorial Hospital in Astoria, Oregon for additional medical care.

6. USCG personnel conducted an inspection and search of the **Vessel**. USCG personnel initially reported discovering twenty-eight (28) seven-gallon jugs containing liquids under a blue canvass on the topside deck of the **Vessel**. USCG personnel conducted two (2) Narcotic Identification Kit (NIK) tests on one of the jugs, both which presumptively tested positive for methamphetamine. USCG also made use of Ion Mobility Spectrometry (also known as an ion scanner), which detected the presence of cocaine on both the **Vessel** and on STIRLING. During the inspection and search, USCG personnel located **Vessel's** official number of 9947859 in the engine compartment

7. The USCG inspection and search of the **Vessel** on the high seas subsequently ceased on April 10, 2019 due to poor weather conditions, crew fatigue and health concerns over the possibility of additional harmful substances on board the **Vessel**. USCG personnel also

determined that a more thorough inspection and search of the **Vessel** could be conducted at port, so USCG determined that the **Vessel** would be towed to port.

8. United States Customs and Border Protection Officer (CBPO) William Wells advised me that he overheard an exchange between STIRLING and a nurse while at Columbia Memorial Hospital. The nurse asked STIRLING what he had taken that caused him to be incapacitated, to which STIRLING replied "Fentanyl," adding that it was a "large amount" that was "pure." STIRLING told the nurse he did it because he realized the Coast Guard was about to board him because he was smuggling. He also stated that he wasn't trying to kill himself by taking the Fentanyl, but that the amount he took was from a "kilo."

9. Due to a paucity of supplies needed to continue administering care to STIRLING, personnel at Columbia Memorial Hospital had STIRLING transported to Adventist Health Portland, a hospital in Portland, Oregon, via ambulance. ICE SA Clifford Jones and I followed the ambulance in my government-owned vehicle (GOV).

10. SA Jones and I met with United States Coast Guard Investigative Service (CGIS) SA Daniel Austin at Adventist Health Portland, whereupon SA Austin remained with STIRLING. SA Austin advised me that he overheard STIRLING tell a doctor that he had consumed fentanyl.

11. SA Jones later relieved SA Austin in observing STIRLING. SA Jones advised me that he overheard a conversation between STIRLING and a nurse. The nurse asked STIRLING if he knew where he was, to which STIRLING responded in the negative. The nurse then asked STIRLING if he knew why he was in the hospital, to which STIRLING said that he got "busted." When the nurse asked what he had been doing, STIRLING stated that he was a drug

smuggler. STIRLING stated that he did not want to go to jail for the rest of his life and that he had a ton of meth and ten (10) loads of fentanyl that he was taking to Canada.

12. A review of STIRLING's criminal history revealed an arrest for conspiracy to import cocaine on or about October 27, 2011. Information received from USCG revealed that STIRLING was interdicted near Columbia in a vessel bound for Australia that contained 381 kilograms of cocaine. On or about February 26, 2013, STIRLING was convicted for importing cocaine and sentenced to ninety (90) months in federal prison.

13. On or about April 11, 2019, USCG personnel moored the **Vessel** to the pier at a USCG Station. USCG personnel retained custody and control of the **Vessel** and the jugs at the USCG Station.

14. After the **Vessel** arrived at the USCG Station, USCG personnel performed a count of the jugs of alleged methamphetamine and discovered that there were in fact twenty-nine (29) jugs, as opposed to the originally reported twenty-eight (28) jugs)

15. On April 18, 2019, the USCG turned custody of the **Vessel** and the twenty-nine (29) jugs of liquid over to Portland ICE personnel at a marine facility on the Multnomah Channel, Portland, Oregon where the **Vessel** is presently located. USCG personnel reported that twenty-eight (28) of the jugs remained on the Vessel, and personally turned over the over (1) jug of liquid used in conducting the NIK tests to ICE personnel.

16. Based on my knowledge, training, and experience, I know that drug traffickers will often maintain firearms on their persons, in their residences, and their conveyances. This is for personal protection, as well as to guard against the theft of their controlled substances and other property.

17. Based on my knowledge, training and experience, I know that drug traffickers often utilize multiple cellular phones. I also know that people travelling on the high seas will possess and use satellite phones, as satellite phones potentially allow for call reception in areas that typically have poor or no service.

18. Based on my knowledge, training and experience, I know that drug traffickers will often maintain books, records, receipts, notes, ledgers, photographs and other documents relating to the manufacture and distribution of controlled substances.

19. Based on my knowledge, training, and experience, I know that drug traffickers will often maintain personal books and papers reflecting names, addresses, telephone numbers, and other contact or identification data relating to the manufacture, importation and distribution of controlled substances.

20. Based on my knowledge, training and experience, I know that drug traffickers will often maintain financial records relating to controlled substances income and expenditures of money and wealth, such as money orders, wire transfer records, cashier's checks and receipts, account records, passbooks, tax records, safe deposit box keys and records, checkbooks, and check registers, as well as precious metals and gems such as gold, silver, diamonds, etc.

21. Based on my knowledge, training, and experience, I know that drug traffickers often maintain documents indicating travel in interstate and foreign commerce, to include airline tickets, notes and travel itineraries; airline schedules; bills; charge card receipts; hotel, motel, and car rental statements; correspondence with travel agencies and other travel related businesses; airline, rent a car, and hotel frequent flier or user cards and statements; passports and visas; telephone bills; photographs of foreign locations; and papers relating to domestic and international travel.

22. SA Austin has informed me that paperwork regarding a vessel's ownership and registration must be maintained in the vessel.

23. Based on my knowledge, training, and experience, I know that drug traffickers will often maintain digital devices and storage media, to include laptop computers, external hard drives, thumb drives, and cameras.

24. Based on information from SA Austin, I know that people operating watercraft such as sailboats, will maintain equipment for piloting, navigating and communicating, to include portable or affixed Global Positioning Satellite (GPS) units, portable or affixed radios, navigational charts, maps, route planning charts, satellite messaging devices, chart plotters, schedules, electronic devices that would log the vessel's position, course, speed, and maritime positioning and store maps.

25. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **Vessel** or inside the **Vessel**, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as "digital devices"). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know that drug traffickers communicate electronically to facilitate drug purchases, schedule "runners," transfer money, arrange the acquisition and delivery of controlled substances, negotiate the price, quality, and quantity of controlled substances, arrange drug stash locations, and receive direction from

drug trafficking organizations, including those operating outside the United States. These digital devices can also store keys to decipher coded terminology.

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

27. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant

but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the **Vessel**, because based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device,

its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is

not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

28. In most cases, a thorough search of a vessel or conveyance for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the **Vessel**, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on or inside the **Vessel** could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different

operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the **Vessel** or at the time of the search of the **Vessel**. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

29. Because other people may share the **Vessel** as a residence, or otherwise have an ownership interest in the **Vessel**, it is possible that the **Vessel** will contain digital devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those digital devices, the warrant applied for would permit the seizure and review of those items as well.

30. Nature of the examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

31. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time

period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

32. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

33. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

34. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

35. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory

evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Conclusion

36. Based on the foregoing, and based on my training and experience, I have probable cause to believe, and do believe, that John Phillip STIRLING knowingly and intentionally possessed with the intent to distribute 500 grams or more of a mixture or substance containing a detectable amount of methamphetamine, a Schedule II controlled substance while on a board a covered vessel, in violation of 46 U.S.C. §§ 70503(a) and 70506(a), and conspired to commit that offense in violation of 46 U.S.C. §70506(b) and that contraband and evidence of the offenses, as described above and in Attachment B, is presently located on the **Vessel**, which is described above and in Attachment A.

37. This affidavit and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Byron Chatfield prior to being submitted to the Court. AUSA Chatfield informed me that in his opinion, the affidavit is legally and factually sufficient to establish probable cause to support the issuance of the search warrant. I therefore request that the Court issue a warrant authorizing a search of the **Vessel** described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

(By phone) JTB

Todd Clements, Special Agent
Immigration and Customs Enforcement

Sworn in accordance with the requirements of Fed. R. Crim P. 4.1 by telephone at 11:20
a.m./p.m. on 4/19/2019.

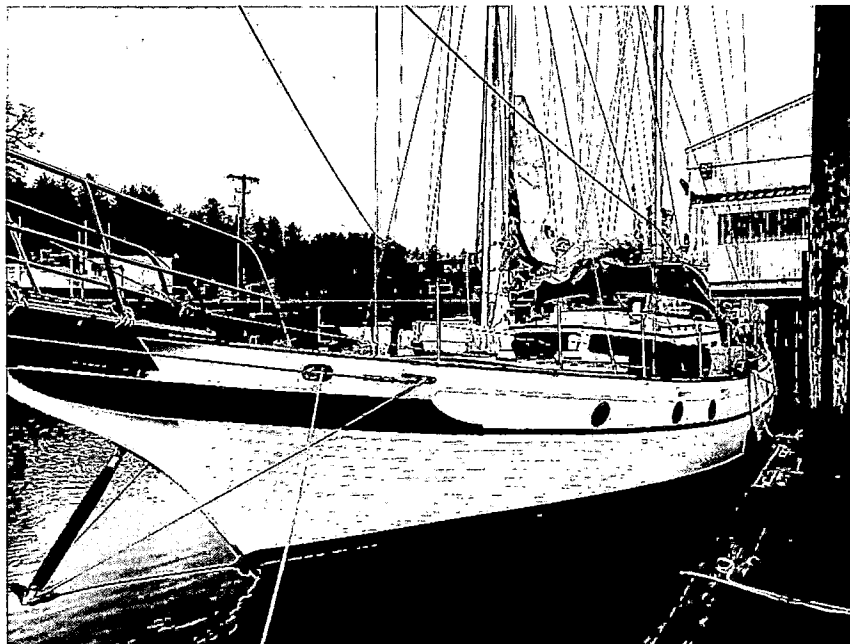
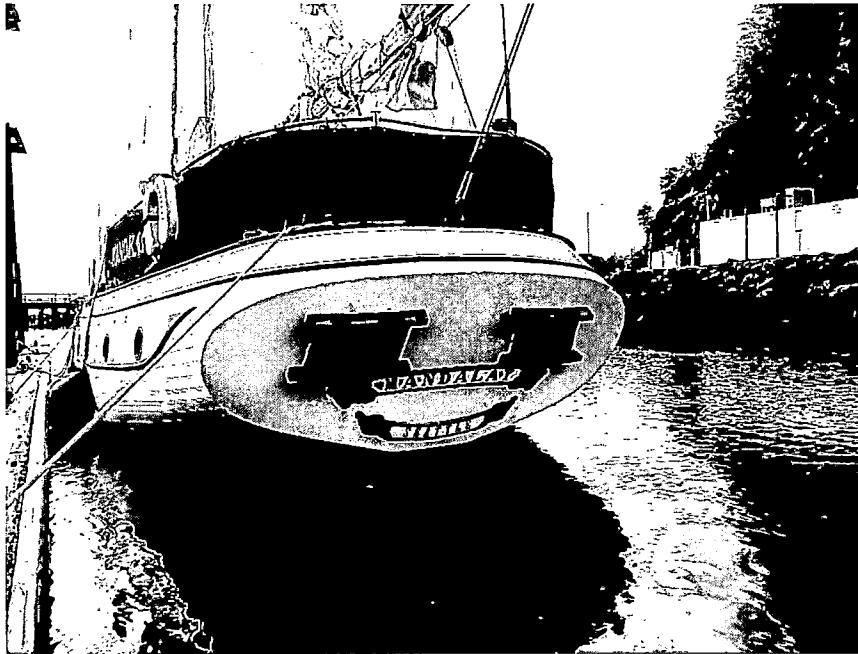
Stacie F. Beckerman

HONORABLE STACIE F. BECKERMAN
U.S. Magistrate Judge, District of Oregon

ATTACHMENT A

Vessel to Be Searched

The vessel to be searched is a white 53.6 foot double-masted sailing vessel with blue trim identified as the Mandalay with Official Number 947859.



ATTACHMENT B**Items to Be Seized**

The items to be searched for, seized, and examined, are those items on the Sailing Vessel (S/V) Mandalay, Official number 947859 (hereinafter **Vessel**), presently located at a marine facility on the Multnomah Channel, Portland, Oregon, referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of 46 U.S.C. §§ 70503(a) and 70506(a) and (b).

1. The items referenced above to be searched for, seized, and examined are as follows:
 - a. Controlled substances, including, but not limited to, fentanyl, cocaine and methamphetamine, held in violation of 46 U.S.C. §§ 70503(a) and 70506(a) and (b);
 - b. Firearms and other dangerous weapons and ammunition;
 - c. Financial profits, proceeds and instrumentalities of trafficking in narcotics and, including U.S. Currency and other items of value purchased/acquired;
 - d. Paraphernalia for packaging, smuggling, processing, diluting, manufacturing, weighing, and distributing controlled substances, for example: hidden compartments, scales, blenders, funnels, sifters, grinders, glass panes, mirrors, razor blades, plastic bags, heat sealing devices, and dilutants such as inositol, vitamin B12, etc.;
 - e. Books, records, receipts, notes, ledgers, photographs, and other documents relating to the manufacture and distribution of controlled substances; communications between members of the conspiracy and evidence of the use of apparently legitimate businesses to disguise profits purchased/acquired;
 - f. Personal books and papers reflecting names, addresses, telephone numbers, and

other contact or identification data relating to the manufacture, importation and distribution of controlled substances;

g. Financial records relating to controlled substances income and expenditures of money and wealth, to wit: money orders, wire transfer records, cashier's checks and receipts, account records, passbooks, tax records, safe deposit box keys and records, checkbooks, and check registers, as well as precious metals and gems such as gold, silver, diamonds, etc.

h. Items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the **Vessel**, including but not limited to vessel registration, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, bills of sale and keys;

i. Documents indicating travel in interstate and foreign commerce, to include airline tickets, notes and travel itineraries; airline schedules; bills; charge card receipts; hotel, motel, and car rental statements; correspondence with travel agencies and other travel related businesses; airline, rent a car, and hotel frequent flier or user cards and statements; passports and visas; telephone bills; photographs of foreign locations; and papers relating to domestic and international travel;

j. Cellular telephones, computers and other electronic devices capable of storing data that constitutes evidence or the instrumentality of drug trafficking;

k. Portable or affixed Global Positioning Satellite (GPS) units, portable or affixed radios, navigational charts, maps, route planning charts, satellite messaging devices, chart plotters, and schedules.

l. Latent prints and identifying material from items in the **Vessel**.